# **Practical Exercise: Fine-Grained Policy Decisions using XACML**

Training Objective

Learn how to use XACML to restrict API exposure.

Business Scenario

PizzaShack wants to implement their own security policies for accessing APIs.

High-Level Steps

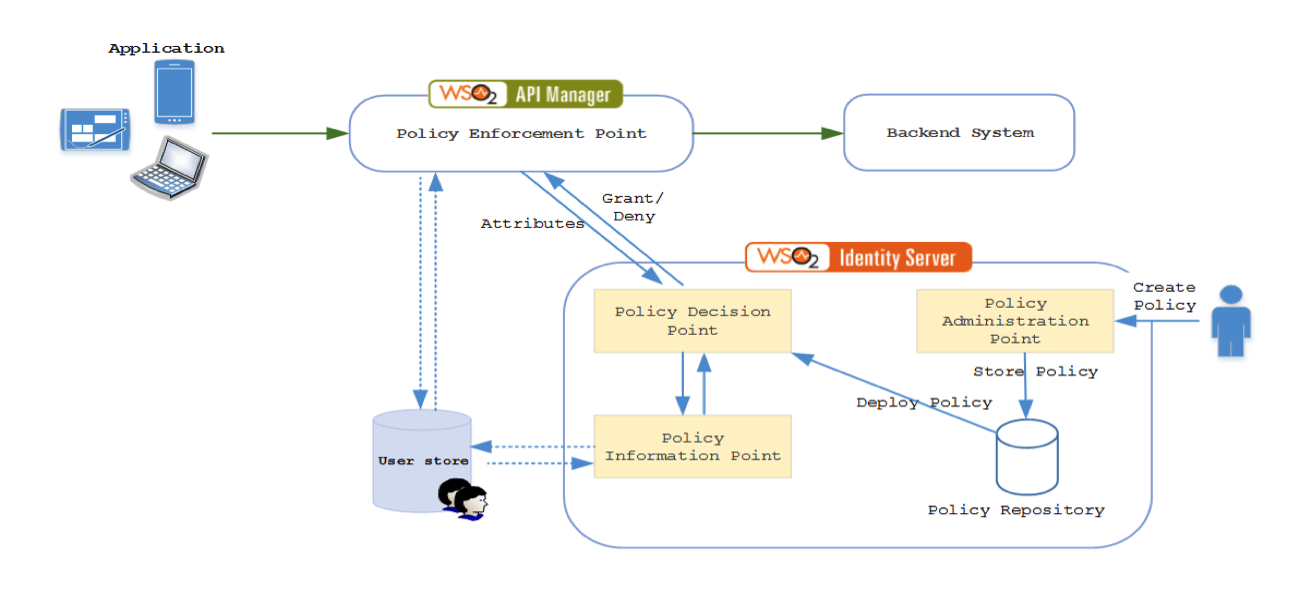
* Install XAML feature in API Manager
* Create policies to restrict API exposure

Detailed Instructions

# **Enabling Role-Based Access Control Using XACML**

### **How XACML is used with WSO2 API Manager**

The diagram shown below depicts the scenario where WSO2 API Manager uses the XACML entitlement server to validate API requests that come into the API Manager. In this case, WSO2 Identity Server has been used as the XACML entitlement server.



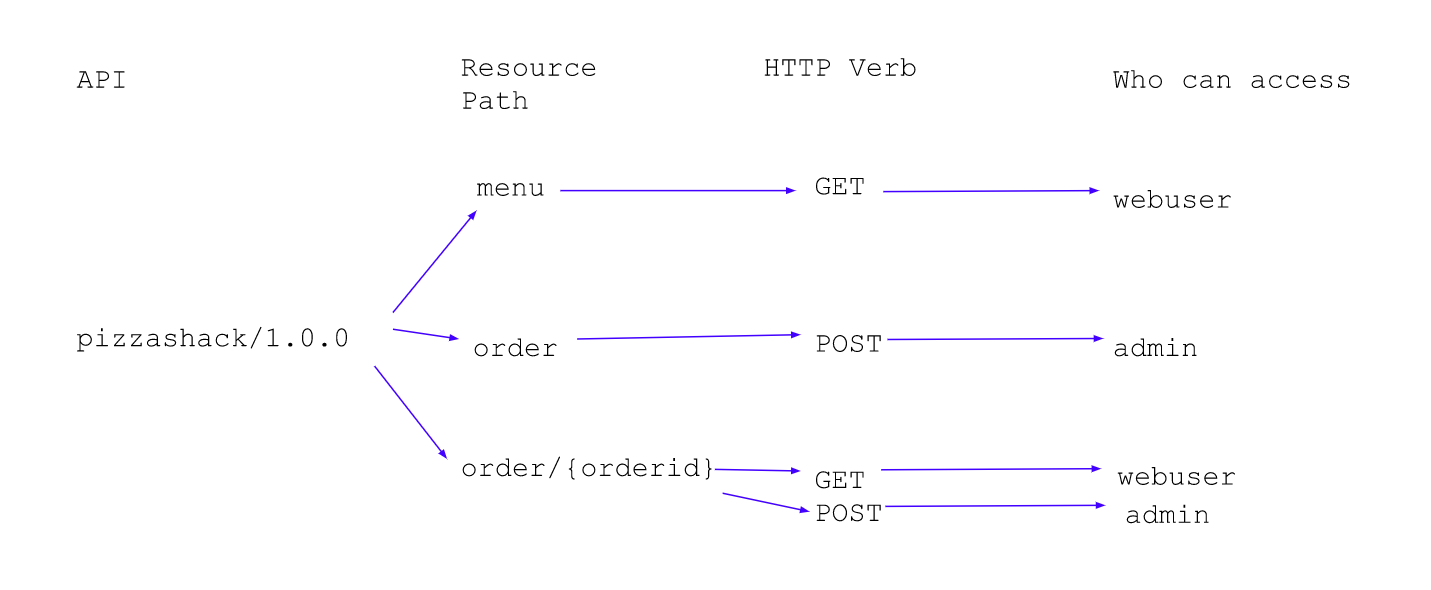
The process is initiated by an administrator who creates the XACML policies and adds them to the PAP. The created policies are stored in a policy repository and promoted to the policy decision point (PDP) by an authorized user. Once the policy is deployed, authorization requests are evaluated against this policy. There can be more than one policy deployed in the PDP.

The API Manager acts as the policy enforcement point (PEP). Whenever an API invocation comes to the API Manager, an authorization request is sent to the PDP with the required attributes. In this case, it can be the name of the user, resource path and the HTTP verb. The PDP receives the request along with these attributes and evaluates the request against the existing policies deployed in the PDP. If the request requires more information, the PDP tries to obtain that information from a policy information point (PIP). In this case, the request from the API Manager can contain the username and the policy that is deployed requires the role of the user. In such a scenario, the PDP gets this information from the user store that is defined as a PIP. Once the PDP has the required information to evaluate the request, a response is sent back to the API Manager with its policy decision.

### **Enabling role-based access control**

The steps below demonstrate how WSO2 Identity Server, acting as a XACML entitlement server, can validate authentication requests from the API Manager based on a set of predefined XACML entitlement policies. This allows a standardized way of defining entitlement policies that can be enforced from WSO2 API Manager. For detailed information on XACML, see [XACML Architecture](https://is.docs.wso2.com/en/5.10.0/get-started/access-control-and-entitlement-management/) in the WSO2 Identity Server documentation.

Let’s take the following requirement in exposing an API via the API manager.



Based on the requirement, a single API is exposed to add or retrieve order information. Each member type (webuser or admin) is identified from the resource path. The operation (GET or POST) that needs to be performed is distinguished by the HTTP verb. Follow the steps below to implement this kind of role-based access control.

1. Let’s start by creating the required users. First, you need to link both the API Manager and the Identity Server to the same user store in order to share users, roles and other related information. This can be done by linking the API manager with the LDAP user store within WSO2 Identity Server. For more information, see [Configuring an external LDAP or Active Directory Userstore](https://apim.docs.wso2.com/en/latest/administer/product-administration/managing-users-and-roles/managing-user-stores/configure-primary-user-store/configuring-a-read-write-ldap-user-store/) . For this you can create a read write LDAP user store.

**Note**

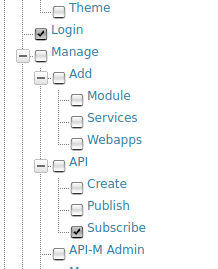
By default, in API Manager JDBCUserStore is enabled. When you are moving to the ReadWriteLDAPUserStore, make sure you have commented the configuration of JDBCUserStore and keep only one user store configuration <API-M\_HOME>/repository/conf/user-mgt.xml in both nodes.

**Tip**

In an actual deployment, both these servers can share the user store of your organization.

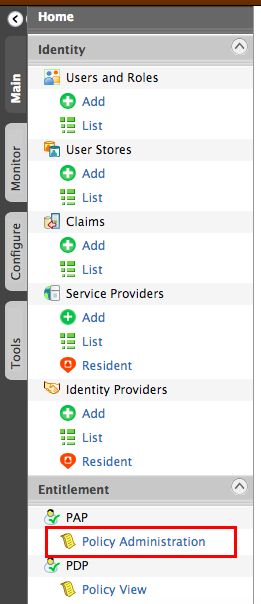
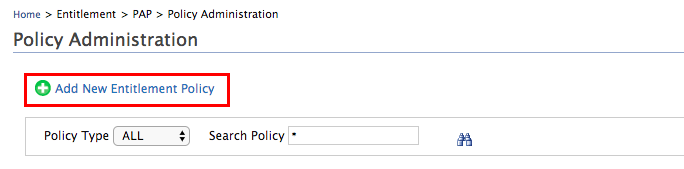
1. Start the WSO2 API Manager server and log in to the Management Console. Create user information with the following permission structure.

| User | Role |
| --- | --- |
| api\_user | webuser |
| api\_admin | admin |

1. When adding the webuser role, set the **Login** and **Subscribe** permissions from permission tree.  
   
2. Start the WSO2 Identity Server and log in to its Admin Console.

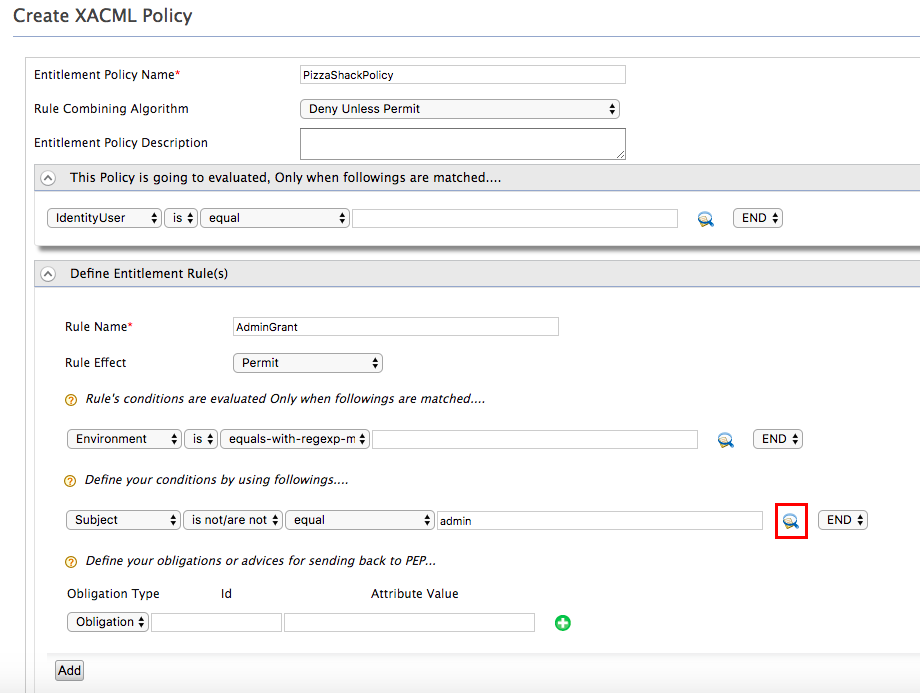
**Tip**

Since API Manager and Identity Server run on the same server, offset the Identity Server by 1.

1. Under the **Entitlement** section, click **Policy Administration > Add New Entitlement Policy** .  
2. You are redirected to a page listing all available policy editors. Select **Standard Policy Editor** from the list and add the values shown below in the policy editor. Refer [Creating a XACML Policy](https://is.docs.wso2.com/en/5.10.0/learn/creating-a-xacml-policy/) in WSO2 Identity Server for more information.
   1. **Entitlement Policy Name:** PizzaShackPolicy
   2. **Rule Combining Algorithm:** Deny unless Permit

When the rule combination algorithm is set to **Deny Unless Permit** , you need to set the permit criteria as a rule.

1. In the **Define Entitlement Rule(s)** area, set the following 2 rules to define the kind of requests and from which user they should be permitted.
   1. AdminGrant - grants full access to the admin user. Give the information below,

**Conditions:** Under **Define your conditions by using followings....** , select drop down options as **Subject** , **is/are** , **at-least-one-member-of** in order and enter **admin** in the last field. Click the icon next to **END** shown below to configure the attribute value and attribute source to retrieve the user roles from the user store. 

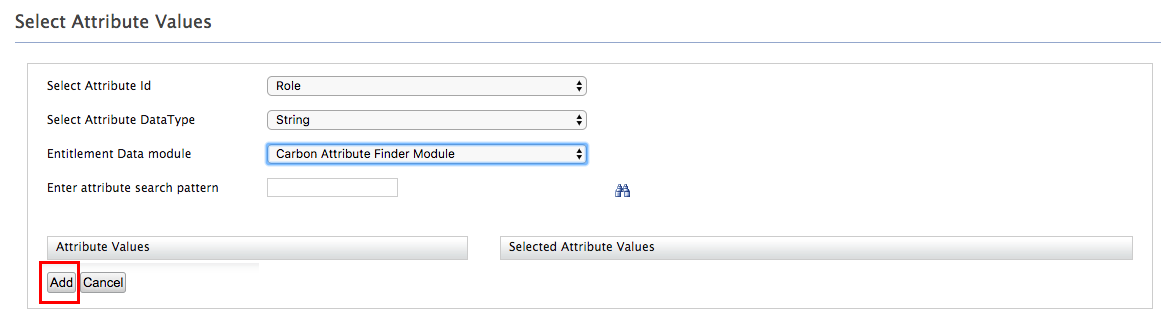
Select the attributes as given below. Note that this needs to be done for all the rules.

**Select Attribute ID:** Role

**Select Attribute Data Type:** String

**Entitlement Data Module:** Carbon Attribute Finder Module

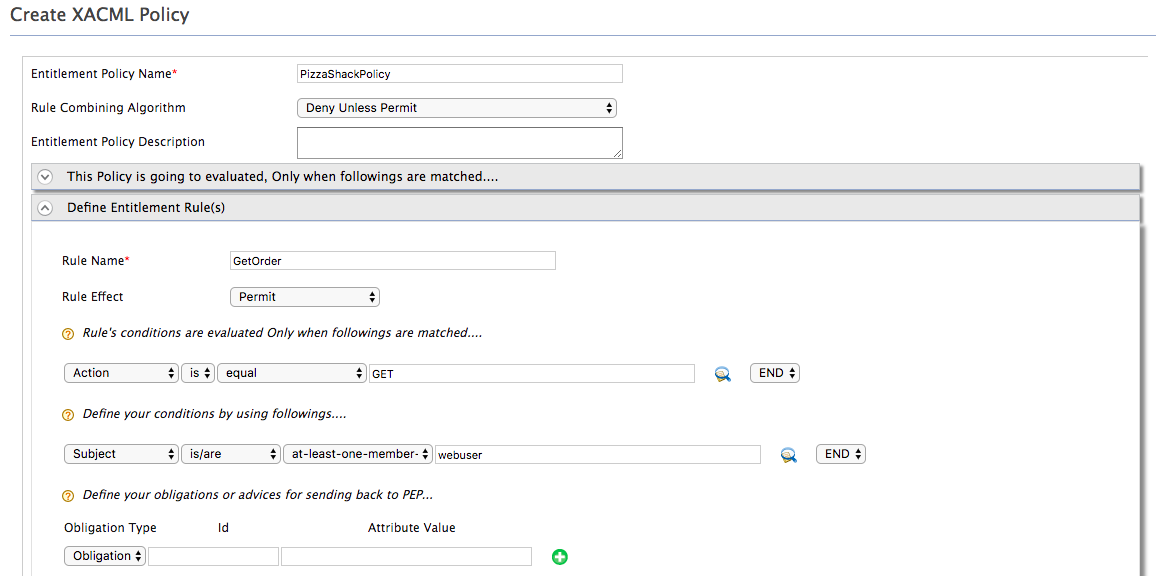
Click on **Add** button after providing above values as shown below.



* 1. GetOrder- allows web users to get order information from the API. Give the information below,

**Rule Name:** GetOrder

**Conditions:** Under **Rule's conditions are evaluated......** , select drop down options as **Action** , **is** , **equal** in order and enter **GET** in the last field. Under **Define your conditions by using followings....** , select drop down options as **Subject** , **is/are** , **at-least-one-member-of** in order and enter **webuser** in the last field. Click the icon next to **END** shown below to configure the attribute value and attribute source to retrieve the user roles from the user store.

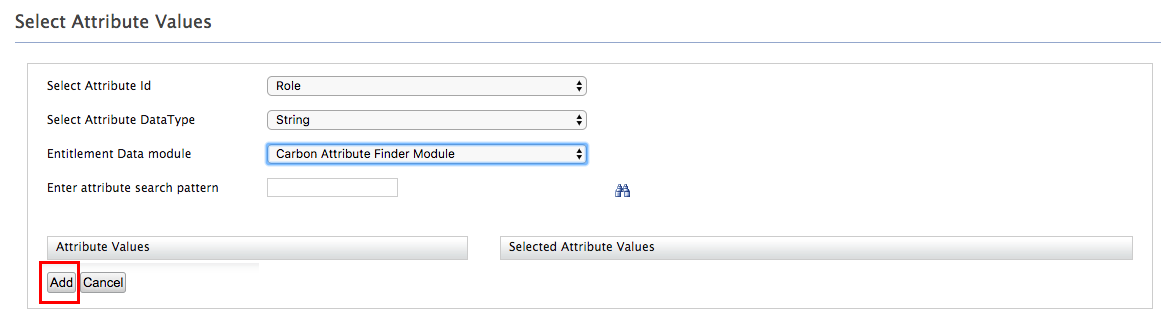


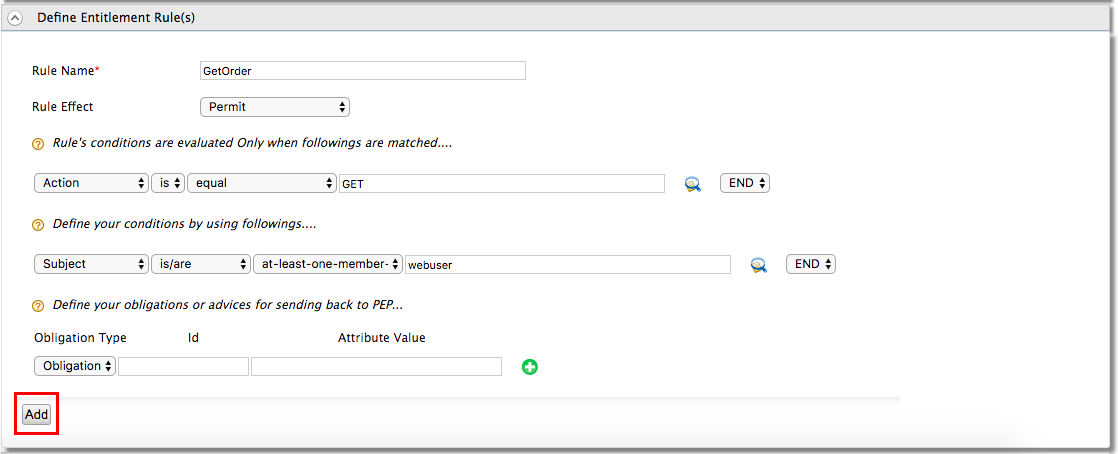
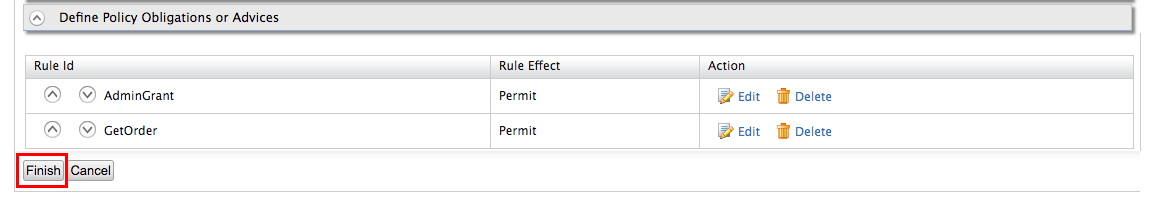
Select the attributes as given below. Note that this needs to be done for all the rules.

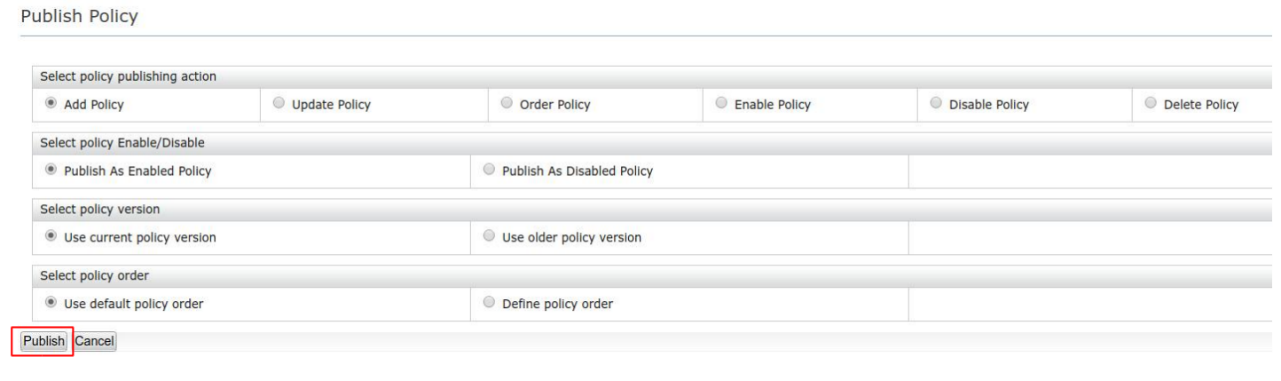
**Select Attribute ID:** Role

**Select Attribute Data Type:** String

**Entitlement Data Module:** Carbon Attribute Finder Module

Click on **Add** button after providing above values as shown below. 

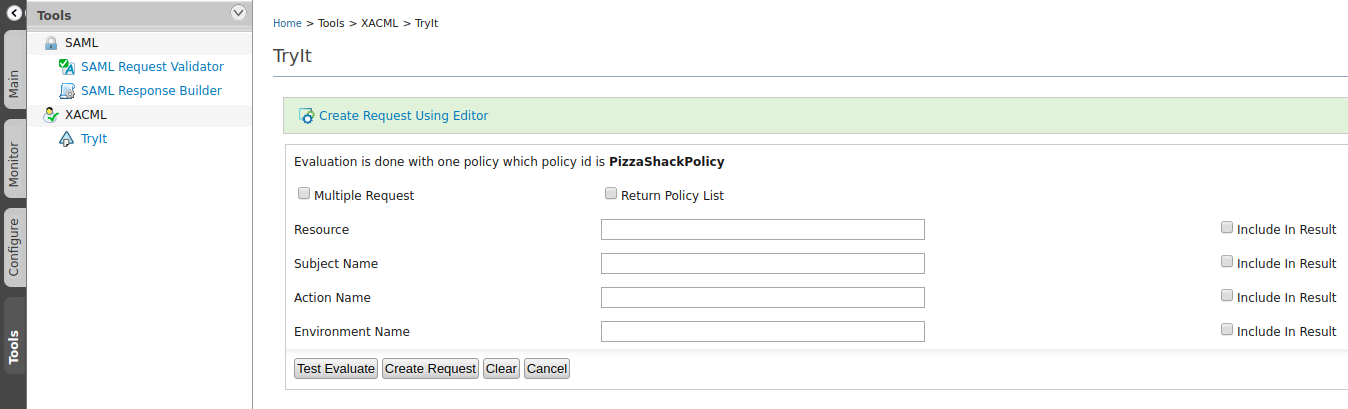
1. Click **Add** once done. 
2. The rules are added to the policy. Click **Finish** to save the policy. 
3. In the Policy Administration page, click **Publish to My PDP** to publish the policy to the PDP.



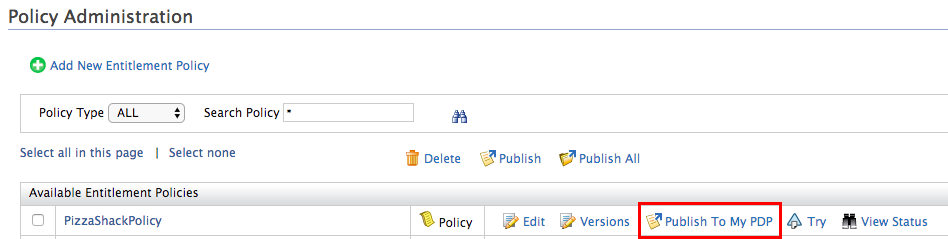
Keep the default selected values in the Publish Policy window and select publish.

**Tip**

You can test the service by clicking **Try** option in front of the entitlement policy. It is the tryIt tool developed for XACML in WSO2 Identity Server and you can access the same tryIt tool by navigating to **Tools > XACML > TryIt** .



You need to enter your username as the **Subject Name** . Refer [Evaluating a XACML Policy](https://is.docs.wso2.com/en/5.10.0/administer/evaluating-a-xacml-policy/) for more information on how to use the TryIt tool for XACML Policy evaluation. For example, try api\_user as the **Subject Name** and GET as the **Action Name**. If the policy is configured correctly, you should get a successful message. Try `POST' as the **Action Name** and you would get a deny message.



1. Download the [entitlement-1.0-SNAPSHOT.jar](https://github.com/nadeesha5814/XACML-APIManager/blob/master/target/entitlement-1.0-SNAPSHOT.jar) and add it to the <API-M\_HOME>/repository/components/lib directory. This JAR file contains the APIEntitlementCallbackHandler class which passes the username, HTTP verb and the resource path to the XACML entitlement server. If you want to view the source code of the JAR, go [here](https://github.com/nadeesha5814/XACML-APIManager) .
2. Restart the server once the JAR file is added.
3. Now, you need to create a API Policy containing the entitlement policy mediator that can be attached to each API required to authorize users with the entitlement server. Create an XML file with the following configuration and name it EntitlementMediator.j2 .

xml <entitlementService xmlns="http://ws.apache.org/ns/synapse" remoteServiceUrl="https://localhost:9444/services" remoteServiceUserName="admin" remoteServicePassword="admin" callbackClass="org.wso2.sample.handlers.entitlement.APIEntitlementCallbackHandler"/>

**Note**

The **Entitlement Mediator** intercepts requests and evaluates the actions performed by a user against an [eXtensible Access Control Markup Language (XACML)](http://en.wikipedia.org/wiki/XACML" \t "_blank) policy. Here, WSO2 Identity Server is used as the XACML Policy Decision Point (PDP) where the policy is set, and WSO2 API Manager serves as the XACML Policy Enforcement Point (PEP) where the policy is enforced. Refer [Entitlement Mediator](https://wso2docs.atlassian.net/wiki/spaces/ESB500/pages/51413335/Entitlement+Mediator) for more information on parameters and usage of this mediator.

**Info**

The attributes in the <entitlementService> element above should be modified according to the services' endpoint configuration as follows.

remoteServiceUrl - Service URL of WSO2 Identity Server, acting as the XACML entitlement server in this scenario.

remoteServiceUserName - Username

remoteServicePassword - Password used to connect to the service

1. Log in to the API Publisher and [create an API](https://apim.docs.wso2.com/en/latest/design/create-api/create-rest-api/create-a-rest-api/). In this sample default PizzaShack API is used.
2. [Create a new API policy](https://apim.docs.wso2.com/en/latest/design/api-policies/create-policy/) and upload the EntitlementMediator.j2 created previously. Set **Request** under the **Applicable flows**
3. Attach the new policy to all the resources as mentioned in [attach policy](https://apim.docs.wso2.com/en/latest/design/api-policies/attach-policy/)
4. Save, deploy, publish and test the API to make sure that the requests specified in the 2 rules defined in step 8 are accessible according to the user role specified. For example, the POST operation is only available to users with the role admin. If an anonymous user tries to access the POST operation, it should fail. Users with webuser role will only be able to access GET resource.

**Note**

If you encounter an error stating "org.apache.axis2.transport.jms.JMSSender cannot be found by axis2\_1.6.1.wso2v16" when publishing the API, comment out the following JMSSender configuration in the <APIM\_HOME>/repository/conf/axis2/axis2\_blocking\_client.xml file and restart the server.

<!--transportSender name="jms" class="org.apache.axis2.transport.jms.JMSSender"/-->

1. If you want to debug the entitlement mediator, enable debug logs in the Management Console for the org.wso2.sample.handlers.entitlement.APIEntitlementCallbackHandler class.

Expected Outcome

API invocation will be restricted according to the policies in place.